PaloAltoNetworks.PCNSA.v2023-03-11.q129

Exam Code:	PCNSA
Exam Name:	Palo Alto Networks Certified Network Security Administrator
Certification Provider:	Palo Alto Networks
Free Question Number:	129
Version:	v2023-03-11
# of views:	4801
# of Questions views:	1290
https://www.freepdfdumps.com/PaloAltoNetworks.PCNSA.v2023-03-11.q129.html	

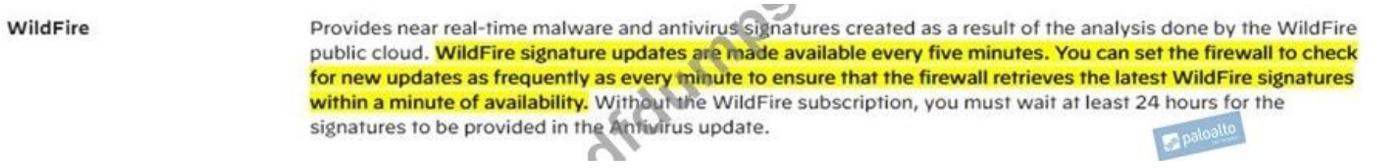
NEW QUESTION: 1
All users from the internal zone must be allowed only HTTP access to a server in the DMZ zone. Complete the empty field in the Security policy using an application object to permit only this type of access.
Source Zone: Internal -
Destination Zone: DMZ Zone -
Application: _____
Service: application-default -
Action: allow
A. Application = "web-browsing"
B. Application = "any"
C. Application = "http"
D. Application = "ssl"
Answer: A (LEAVE A REPLY)

NEW QUESTION: 2
Which attribute can a dynamic address group use as a filtering condition to determine its membership?
A. tag
B. wildcard mask
C. IP address
D. subnet mask
Answer: A (LEAVE A REPLY)
Dynamic Address Groups: A dynamic address group populates its members dynamically using looks ups for tags and tag-based filters. Dynamic address groups are very useful if you have an extensive virtual infrastructure where changes in virtual machine location/IP address are frequent. For example, you have a sophisticated failover setup or provision new virtual machines frequently

and would like to apply policy to traffic from or to the new machine without modifying the configuration/rules on the firewall.
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects-address-groups

NEW QUESTION: 3
Which rule type is appropriate for matching traffic both within and between the source and destination zones?
A. intrazone
B. shadowed
C. universal
D. interzone
Answer: D (LEAVE A REPLY)

NEW QUESTION: 4
What in the minimum frequency for which you can configure the firewall too check for new wildfire antivirus signatures?
A. every 5 minutes
B. every 1 minute
C. every 24 hours
D. every 30 minutes
Answer: (SHOW ANSWER)


WildFire

Provides near real-time malware and antivirus signatures created as a result of the analysis done by the WildFire public cloud. **WildFire signature updates are made available every five minutes. You can set the firewall to check for new updates as frequently as every minute to ensure that the firewall retrieves the latest WildFire signatures within a minute of availability.** Without the WildFire subscription, you must wait at least 24 hours for the signatures to be provided in the Antivirus update.

paloalto

NEW QUESTION: 5
A Security Profile can block or allow traffic at which point?
A. after it is matched to a Security policy rule that allows traffic
B. on either the data plane or the management plane
C. after it is matched to a Security policy rule that allows or blocks traffic
D. before it is matched to a Security policy rule
Answer: A (LEAVE A REPLY)

NEW QUESTION: 6
The firewall sends employees an application block page when they try to access Youtube.
Which Security policy rule is blocking the youtube application?

			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

A. interzone-default
B. Deny Google
C. allowed-security services
D. intrazone-default
Answer: A (LEAVE A REPLY)

NEW QUESTION: 7
Which solution is a viable option to capture user identification when Active Directory is not in use?
A. Authentication Portal
B. group mapping
C. Directory Sync Service
D. Cloud Identity Engine
Answer: A (LEAVE A REPLY)

NEW QUESTION: 8
Which three statement describe the operation of Security Policy rules or Security Profiles? (Choose three)
A. Security Profile should be used only on allowed traffic.
B. Security Profile are attached to security policy rules.
C. Security policy rules inspect but do not block traffic.
D. Security Policy rules can block or allow traffic.
E. Security Policy rules are attached to Security Profiles.
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 9
Which component is a building block in a Security policy rule?
A. decryption profile
B. destination interface
C. timeout (min)
D. application
Answer: (SHOW ANSWER)
Explanation/Reference:

Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/policies/policies-security/buildingblocks-in-a-security-policy-rule.html

NEW QUESTION: 10
Which security profile will provide the best protection against ICMP floods, based on individual combinations of a packet`s source and destination IP address?
A. DoS protection
B. URL filtering
C. anti-spyware
D. packet buffering
Answer: A (LEAVE A REPLY)

NEW QUESTION: 11
A website is unexpectedly allowed due to miscategorization.
What are two ways to resolve this issue for a proper response? (Choose two.)
A. Identify the URL category being assigned to the website.
Edit the active URL Filtering profile and update that category's site access settings to block.
B. Create a URL category and assign the affected URL.
Update the active URL Filtering profile site access setting for the custom URL category to block.
C. Create a URL category and assign the affected URL.
Add a Security policy with a URL category qualifier of the custom URL category below the original policy. Set the policy action to Deny.
D. Review the categorization of the website on https://urlfiltering.paloaltonetworks.com.
Submit for "request change*, identifying the appropriate categorization, and wait for confirmation before testing again.
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Which two features can be used to tag a username so that it is included in a dynamic user group? (Choose two.)
A. XML API
B. GlobalProtect agent
C. User-ID Windows-based agent
D. log forwarding auto-tagging
Answer: (SHOW ANSWER)

NEW QUESTION: 13
An administrator would like to apply a more restrictive Security profile to traffic for file sharing applications. The administrator does not want to update the Security policy or object when new applications are released.

Which object should the administrator use as a match condition in the Security policy?

A. the Online Storage and Backup URL category

B. an application group containing all of the file-sharing App-IDs reported in the traffic logs

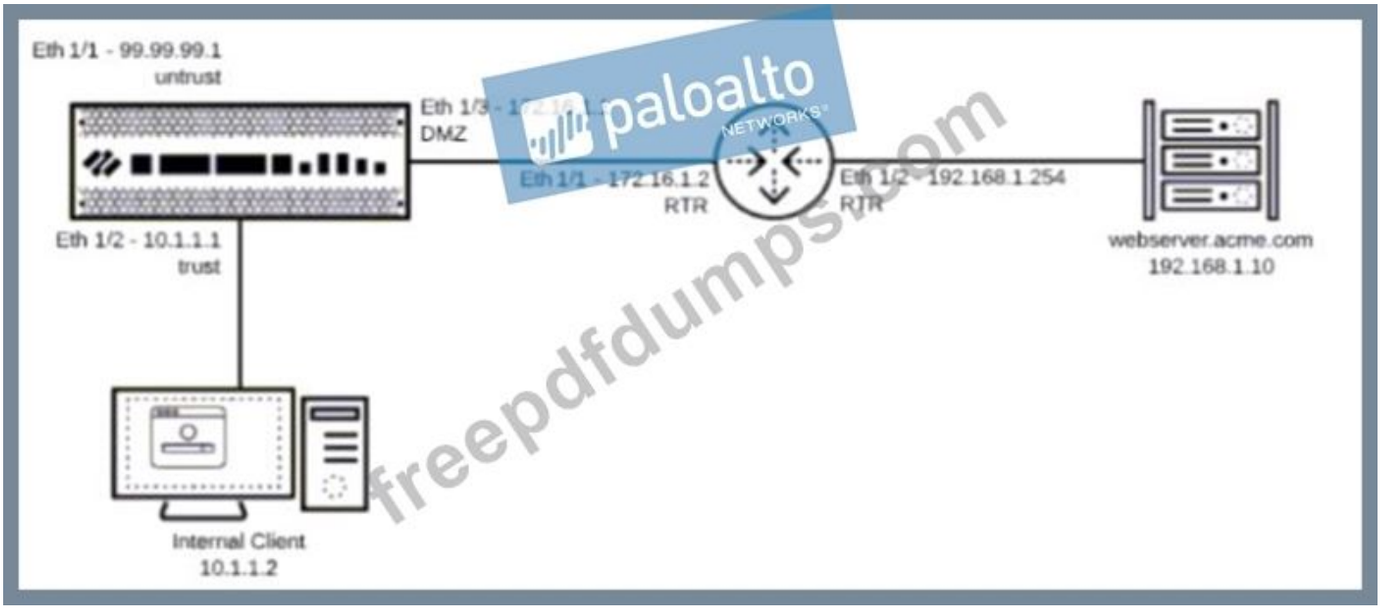
C. the Content Delivery Networks URL category

D. an application filter for applications whose subcategory is file-sharing

Answer: D (LEAVE A REPLY)

NEW QUESTION: 14

You have been tasked to configure access to a new web server located in the DMZ Based on the diagram what configuration changes are required in the NGFW virtual router to route traffic from the 10 1 1 0/24 network to 192 168 1 0/24?



A. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with a next-hop of 192.168 1.10

B. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/2 with a next-hop of 172.16.1.2

C. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with a next-hop of 172.16.1.2

D. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with a next-hop of 192.168.1.254

Answer: C (LEAVE A REPLY)

NEW QUESTION: 15

Which three configuration settings are required on a Palo Alto networks firewall management interface?

A. default gateway

B. netmask

C. IP address

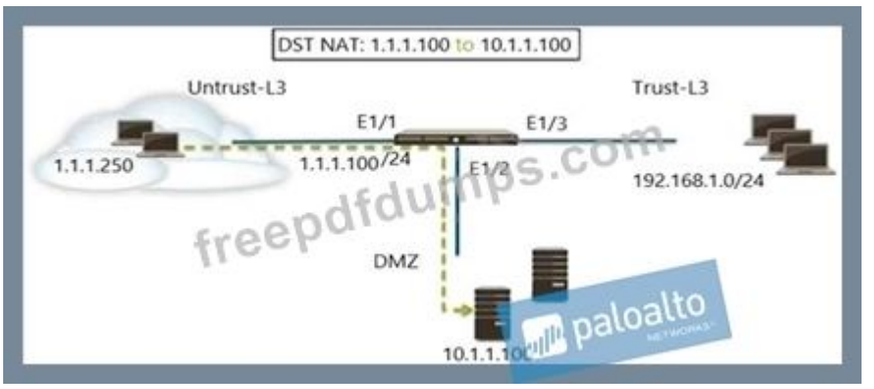
D. hostname

E. auto-negotiation
Answer: A,B,C (LEAVE A REPLY)
Explanation/Reference:
Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClN7CAK

NEW QUESTION: 16
Which Security policy match condition would an administrator use to block traffic from IP addresses on the Palo Alto Networks EDL of Known Malicious IP Addresses list?
A. destination address
B. source address
C. destination zone
D. source zone
Answer: B (LEAVE A REPLY)

NEW QUESTION: 17
Assume a custom URL Category Object of "NO-FILES" has been created to identify a specific website How can file uploading/downloading be restricted for the website while permitting general browsing access to that website?
A. Create a Security policy with a URL Filtering profile that references the site access setting of block to NO-FILES
B. Create a Security policy that references NO-FILES as a URL Category qualifier, with an appropriate Data Filtering profile
C. Create a Security policy with a URL Filtering profile that references the site access setting of continue to NO-FILES
D. Create a Security policy that references NO-FILES as a URL Category qualifier, with an appropriate File Blocking profile
Answer: A (LEAVE A REPLY)

NEW QUESTION: 18
Refer to the exhibit. A web server in the DMZ is being mapped to a public address through DNAT.



Which Security policy rule will allow traffic to flow to the web server?

A. Untrust (any) to DMZ (1.1.1.100), web browsing - Allow

B. Untrust (any) to DMZ (10.1.1.100), web browsing -Allow

C. Untrust (any) to Untrust (10.1.1.100), web browsing -Allow

D. Untrust (any) to Untrust (1.1.1.100), web browsing - Allow

Answer: A (LEAVE A REPLY)

NEW QUESTION: 19

Selecting the option to revert firewall changes will replace what settings?

A. The device state with settings from another configuration

B. The running configuration with settings from the candidate configuration

C. The candidate configuration with settings from the running configuration

D. Dynamic update scheduler settings

Answer: B (LEAVE A REPLY)

NEW QUESTION: 20

An administrator would like to determine the default deny action for the application dns-over-https

Which action would yield the information?

A. Check the action for the decoder in the antivirus profile

B. View the application details in Objects > Applications

C. Check the action for the Security policy matching that traffic

D. View the application details in beacon paloaltonetworks.com

Answer: A (LEAVE A REPLY)

NEW QUESTION: 21

Which action results in the firewall blocking network traffic with out notifying the sender?

A. Reset Server

B. Drop

C. Deny

D. Reset Client

Answer: C (LEAVE A REPLY)

NEW QUESTION: 22

Starting with PAN-OS version 9.1, application dependency information is now reported in which two locations? (Choose two.)

A. on the Policy Optimizer's Rule Usage page

B. on the Application tab in the Security Policy Rule creation window

C. on the Objects > Applications browser pages

D. on the App Dependency tab in the Commit Status window

Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 23

An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration.

Why doesn't the administrator see the traffic?

A. Logging on the interzone-default policy is disabled

B. The Log Forwarding profile is not configured on the policy.

C. The interzone-default policy is disabled by default

D. Traffic is being denied on the interzone-default policy.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 24

An administrator is reviewing the Security policy rules shown in the screenshot below.

Which statement is correct about the information displayed?

A. The view Rulebase as Groups is checked.

B. Eleven rules use the "Infrastructure* tag.

C. Highlight Unused Rules is checked.

D. There are seven Security policy rules on this firewall.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 25

Which interface type is used to monitor traffic and cannot be used to perform traffic shaping?

A. Layer 3

B. Virtual Wire
C. Tap
D. Layer 2
Answer: C (LEAVE A REPLY)

NEW QUESTION: 26
Which statement best describes the use of Policy Optimizer?
A. Policy Optimizer can add or change a Log Forwarding profile for each Secunty policy selected
B. Policy Optimizer on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications
C. Policy Optimizer can display which Security policies have not been used in the last 90 days
D. Policy Optimizer can be used on a schedule to automatically create a disabled Layer 7 App-ID Security policy for every Layer 4 policy that exists Admins can then manually enable policies they want to keep and delete ones they want to remove
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Which option lists the attributes that are selectable when setting up an Application filters?
A. Category, Subcategory, Technology, and Characteristic
B. Category, Subcategory, Technology, Risk, and Characteristic
C. Name, Category, Technology, Risk, and Characteristic
D. Category, Subcategory, Risk, Standard Ports, and Technology
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Reference:
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/objects/objects-application- filters

NEW QUESTION: 28
How is the hit count reset on a rule?
A. select a security policy rule, right click Hit Count > Reset
B. in the CLI, type command reset hitcount <POLICY-NAME>
C. with a dataplane reboot
D. Device > Setup > Logging and Reporting Settings > Reset Hit Count
Answer: A (LEAVE A REPLY)

NEW QUESTION: 29
An administrator wishes to follow best practices for logging traffic that traverses the firewall Which log setting is correct?
A. Disable all logging
B. Enable Log at Session End

C. Enable Log at Session Start
D. Enable Log at both Session Start and End
Answer: B (LEAVE A REPLY)
Explanation
Explanation/Reference:
Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clt5CAC

NEW QUESTION: 30
A server-admin in the USERS-zone requires SSH-access to all possible servers in all current and future Public Cloud environments. All other required connections have already been enabled between the USERS- and the OUTSIDE-zone. What configuration-changes should the Firewall-admin make?
A. Create a security-rule that allows traffic from zone USERS to OUTSIDE to allow traffic from any source IP-address to any destination IP-address for application SSH
B. In addition to option a, a custom-service-object called SERVICE-SSH-RETURN that contains source-port-TCP-22 should be created. A second security-rule is required that allows traffic from zone OUTSIDE to USERS for SERVICE-SSH-RETURN for any source-IP-address to any destination-Ip-address
C. In addition to option c, an additional rule from zone OUTSIDE to USERS for application SSH from any source-IP-address to any destination-IP-address is required to allow the return-traffic from the SSH-servers to reach the server-admin
D. Create a custom-service-object called SERVICE-SSH for destination-port-TCP-22. Create a security-rule between zone USERS and OUTSIDE to allow traffic from any source IP-address to any destination IP-address for SERVICE-SSH
Answer: A (LEAVE A REPLY)

NEW QUESTION: 31
An administrator needs to allow users to use only certain email applications.
How should the administrator configure the firewall to restrict users to specific email applications?
A. Create an application filter and filter it on the collaboration category, email subcategory.
B. Create an application filter and filter it on the collaboration category.
C. Create an application group and add the email applications to it.
D. Create an application group and add the email category to it.
Answer: (SHOW ANSWER)

NEW QUESTION: 32
Based on the show security policy rule would match all FTP traffic from the inside zone to the outside zone?

A. internal-inside-dmz
B. inside-portal
C. engress outside
D. intercone-default
Answer: C (LEAVE A REPLY)

NEW QUESTION: 33
An administrator needs to allow users to use their own office applications. How should the administrator configure the firewall to allow multiple applications in a dynamic environment?
A. Create an Application Filter and name it Office Programs, the filter it on the business-systems category, office-programs subcategory
B. Create an Application Group and add business-systems to it
C. Create an Application Filter and name it Office Programs, then filter it on the business-systems category
D. Create an Application Group and add Office 365, Evernote, Google Docs, and Libre Office
Answer: (SHOW ANSWER)
An application filter is an object that dynamically groups applications based on application attributes that you define, including category, subcategory, technology, risk factor, and characteristic. This is useful when you want to safely enable access to applications that you do not explicitly sanction, but that you want users to be able to access. For example, you may want to enable employees to choose their own office programs (such as Evernote, Google Docs, or Microsoft Office 365) for business use. To safely enable these types of applications, you could create an application filter that matches on the Category business-systems and the Subcategory office-programs. As new applications office programs emerge and new App-IDs get created,

these new applications will automatically match the filter you defined; you will not have to make any additional changes to your policy rulebase to safely enable any application that matches the attributes you defined for the filter.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/use-application-objects-in -policy/create-an-application-filter.html

NEW QUESTION: 34
What are three valid ways to map an IP address to a username? (Choose three.)
A. a user connecting into a GlobalProtect gateway using a GlobalProtect Agent
B. WildFire verdict reports
C. DHCP Relay logs
D. using the XML API
E. usernames inserted inside HTTP Headers
Answer: (SHOW ANSWER)

NEW QUESTION: 35
URL categories can be used as match criteria on which two policy types? (Choose two.)
A. authentication
B. NAT
C. decryption
C application override
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 36
An administrator is trying to enforce policy on some (but not all) of the entries in an external dynamic list. What is the maximum number of entries that they can be exclude?
A. 200
B. 50
C. 100
D. 1,000
Answer: C (LEAVE A REPLY)

NEW QUESTION: 37
An administrator wants to create a NAT policy to allow multiple source IP addresses to be translated to the same public IP address. What is the most appropriate NAT policy to achieve this?
A. Destination
B. Dynamic IP and Port
C. Static IP
D. Dynamic IP
Answer: B (LEAVE A REPLY)

NEW QUESTION: 38
Which Palo Alto network security operating platform component provides consolidated policy creation and centralized management?
A. GlobalProtect
B. AutoFocus
C. Prisma SaaS
D. Panorama
Answer: D (LEAVE A REPLY)

NEW QUESTION: 39
What is the correct process tor creating a custom URL category?
A. Objects > Security Profiles > URL Category > Add
B. Objects > Custom Objects > URL Category > Add
C. Objects > Custom Objects > URL Filtering > Add
D. Objects > Security Profiles > URL Filtering > Add
Answer: (SHOW ANSWER)

NEW QUESTION: 40
An administrator would like to override the default deny action for a given application and instead would like to block the traffic and send the ICMP code "communication with the destination is administratively prohibited" Which security policy action causes this?
A. Drop
B. Reset server
C. Reset both
D. Drop, send ICMP Unreachable
Answer: D (LEAVE A REPLY)

NEW QUESTION: 41
Which action would an administrator take to ensure that a service object will be available only to the selected device group?
A. create the service object in the specific template
B. uncheck the shared option
C. ensure that disable override is selected
D. ensure that disable override is cleared
Answer: D (LEAVE A REPLY)
https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-firewalls/manage-device-groups/create-objects-for-use-in-shared-or-device-group-policy

NEW QUESTION: 42

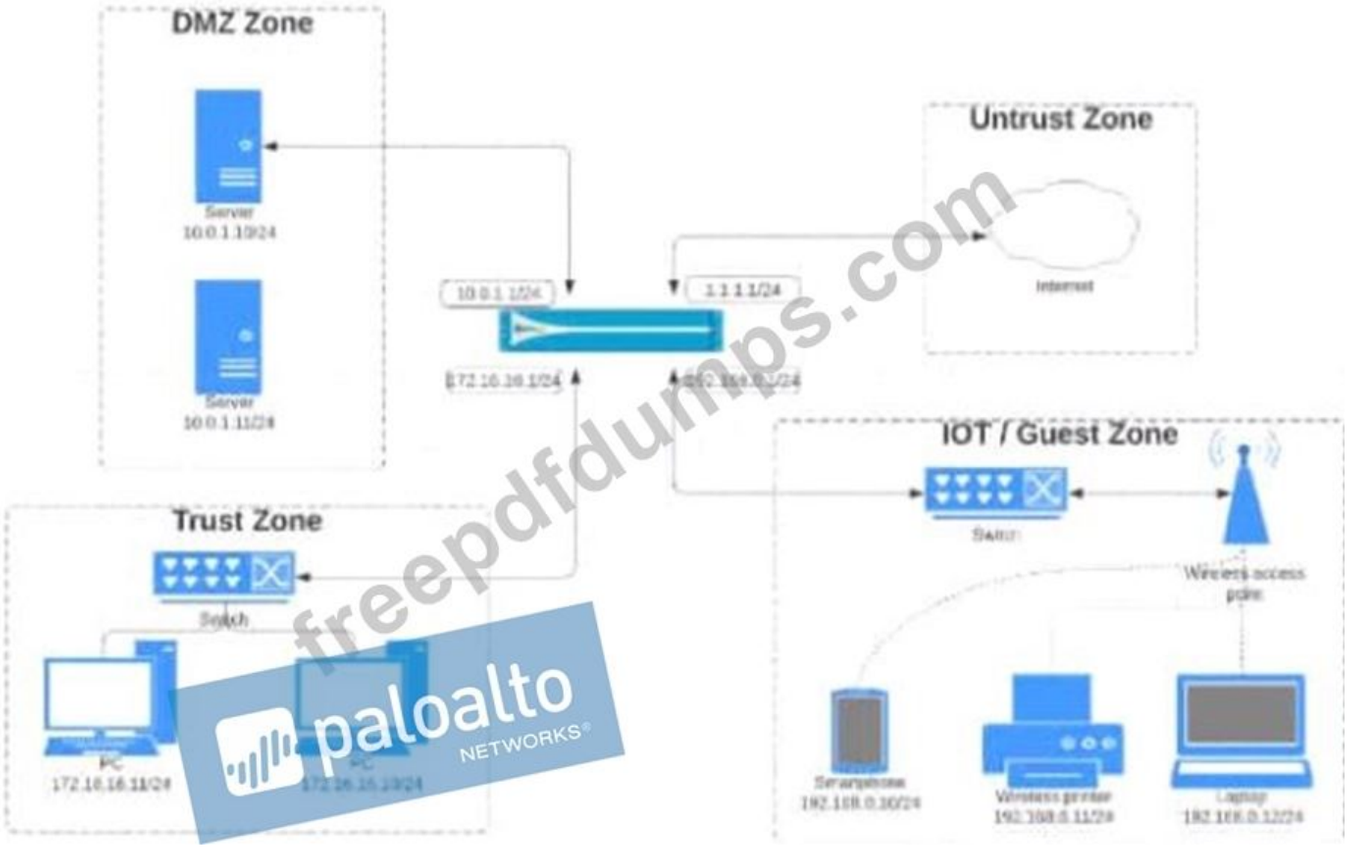
How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?
A. Automatically "download and install" but with the "disable new applications" option used
B. Disable automatic updates during weekdays
C. Automatically "download only" and then install Applications and Threats later, after the administrator approves the update
D. Configure the option for "Threshold"
Answer: D (LEAVE A REPLY)

NEW QUESTION: 43
An administrator has configured a Security policy where the matching condition includes a single application and the action is deny If the application s default deny action is reset-both what action does the firewall take*?
A. It sends a TCP reset to the server-side device
B. It sends a TCP reset to the client-side and server-side devices
C. It silently drops the traffic and sends an ICMP unreachable code
D. It silently drops the traffic
Answer: B (LEAVE A REPLY)

NEW QUESTION: 44
Which data flow direction is protected in a zero trust firewall deployment that is not protected in a perimeter-only firewall deployment?
A. north south
B. outbound
C. east west
D. inbound
Answer: C (LEAVE A REPLY)

NEW QUESTION: 45
Starting with PAN_OS version 9.1 which new type of object is supported for use within the user field of a security policy rule?
A. dynamic user group
B. remote username
C. static user group
D. local username
Answer: A (LEAVE A REPLY)

NEW QUESTION: 46
View the diagram.



What is the most restrictive yet fully functional rule to allow general Internet and SSH traffic into both the DMZ and Untrust/Internet zones from each of the IOT/Guest and Trust Zones?

A)

B)

C)

A. Option A

B. Option B
C. Option C
D. Option D
Answer: C (LEAVE A REPLY)

NEW QUESTION: 47
Which statement is true regarding a Prevention Posture Assessment?
A. It provides a percentage of adoption for each assessment area
B. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture
C. The Security Policy Adoption Heatmap component filters the information by device groups, serial numbers, zones, areas of architecture, and other categories
D. It performs over 200 security checks on Panorama/firewall for the assessment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 48
Based on the screenshot presented which column contains the link that when clicked opens a window to display all applications matched to the policy rule?

A. Apps Seen
B. Name
C. Service
D. Apps Allowed
Answer: A (LEAVE A REPLY)

NEW QUESTION: 49

Which Security profile can you apply to protect against malware such as worms and Trojans?
A. data filtering
B. antivirus
C. vulnerability protection
D. anti-spyware
Answer: B (LEAVE A REPLY)
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles#:~:text=Antivirus%20profiles%20protect%20against%20viruses,as%20well%20as%20spyware%20downloads

NEW QUESTION: 50
The CFO found a USB drive in the parking lot and decide to plug it into their corporate laptop. The USB drive had malware on it that loaded onto their computer and then contacted a known command and control (CnC) server, which ordered the infected machine to begin Exfiltrating data from the laptop.
Which security profile feature could have been used to prevent the communication with the CnC server?
A. Create an anti-spyware profile and enable DNS Sinkhole
B. Create an antivirus profile and enable DNS Sinkhole
C. Create a URL filtering profile and block the DNS Sinkhole category
D. Create a security policy and enable DNS Sinkhole
Answer: A (LEAVE A REPLY)
References:

NEW QUESTION: 51
Which file is used to save the running configuration with a Palo Alto Networks firewall?
A. running-configuration.xml
B. run-config.xml
C. run-configuratin.xml
D. running-config.xml
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Given the image, which two options are true about the Security policy rules. (Choose two.)

				Source				Destination		Rule Usage						
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application	Service	Action	Profile
1	Allow Office Programs	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	Office-program	Application-d...	Allow	None
2	Allow FTP to web ser..	None	Universal	Inside	Any	Any	Any	Outside	ftp-server	-	-	-	any	ftp-service..	Allow	None
3	Allow Social Networkin..	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	facebook	Application-d...	Allow	None

A. The Allow Office Programs rule is using an Application Filter

B. In the Allow FTP to web server rule, FTP is allowed using App-ID

C. The Allow Office Programs rule is using an Application Group

D. In the Allow Social Networking rule, allows all of Facebook's functions

Answer: A,D (LEAVE A REPLY)

In the Allow FTP to web server rule, FTP is allowed using port based rule and not APP-ID.

NEW QUESTION: 53

When is the content inspection performed in the packet flow process?

A. before the packet forwarding process

B. before session lookup

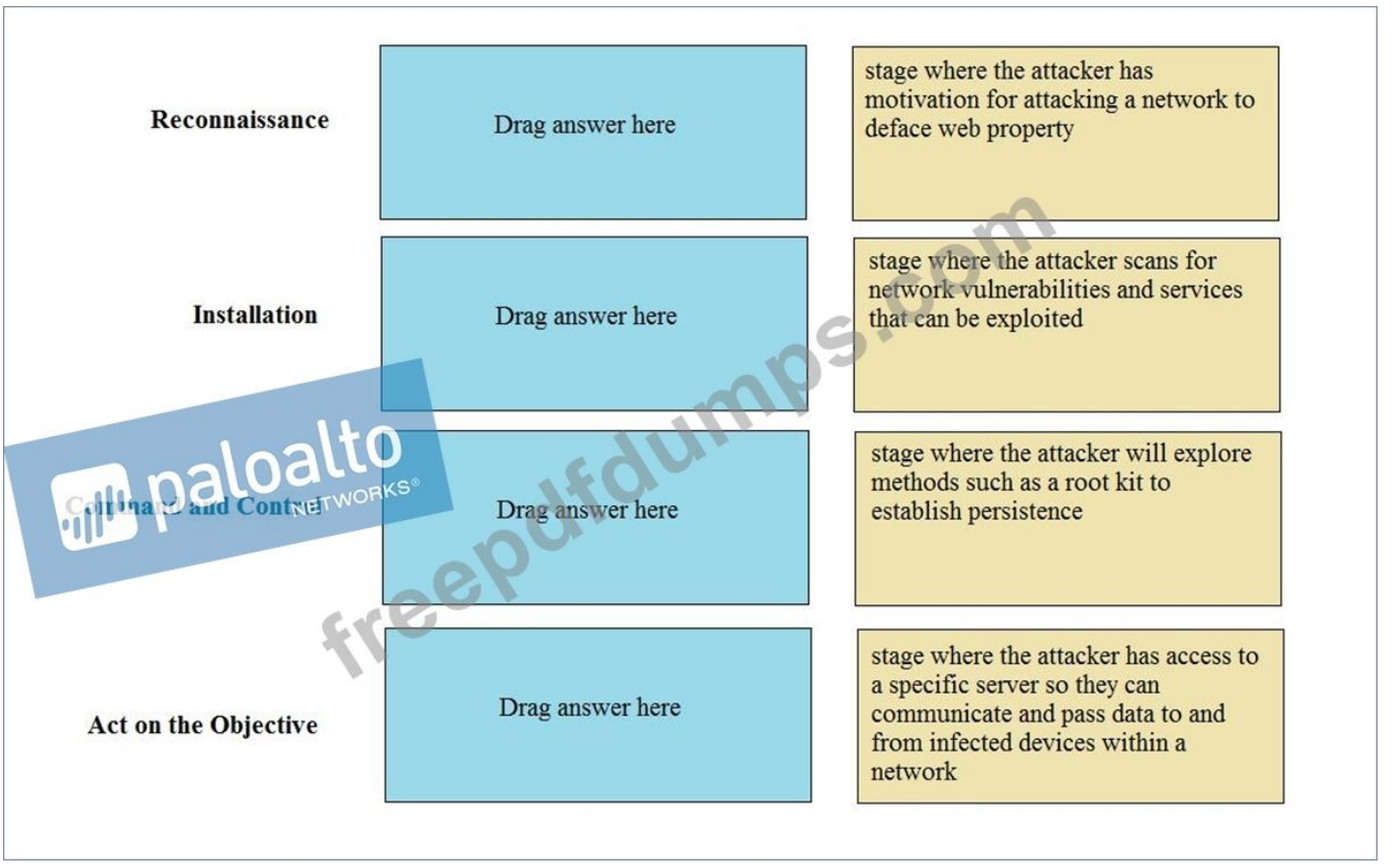
C. after the application has been identified

D. after the SSL Proxy re-encrypts the packet

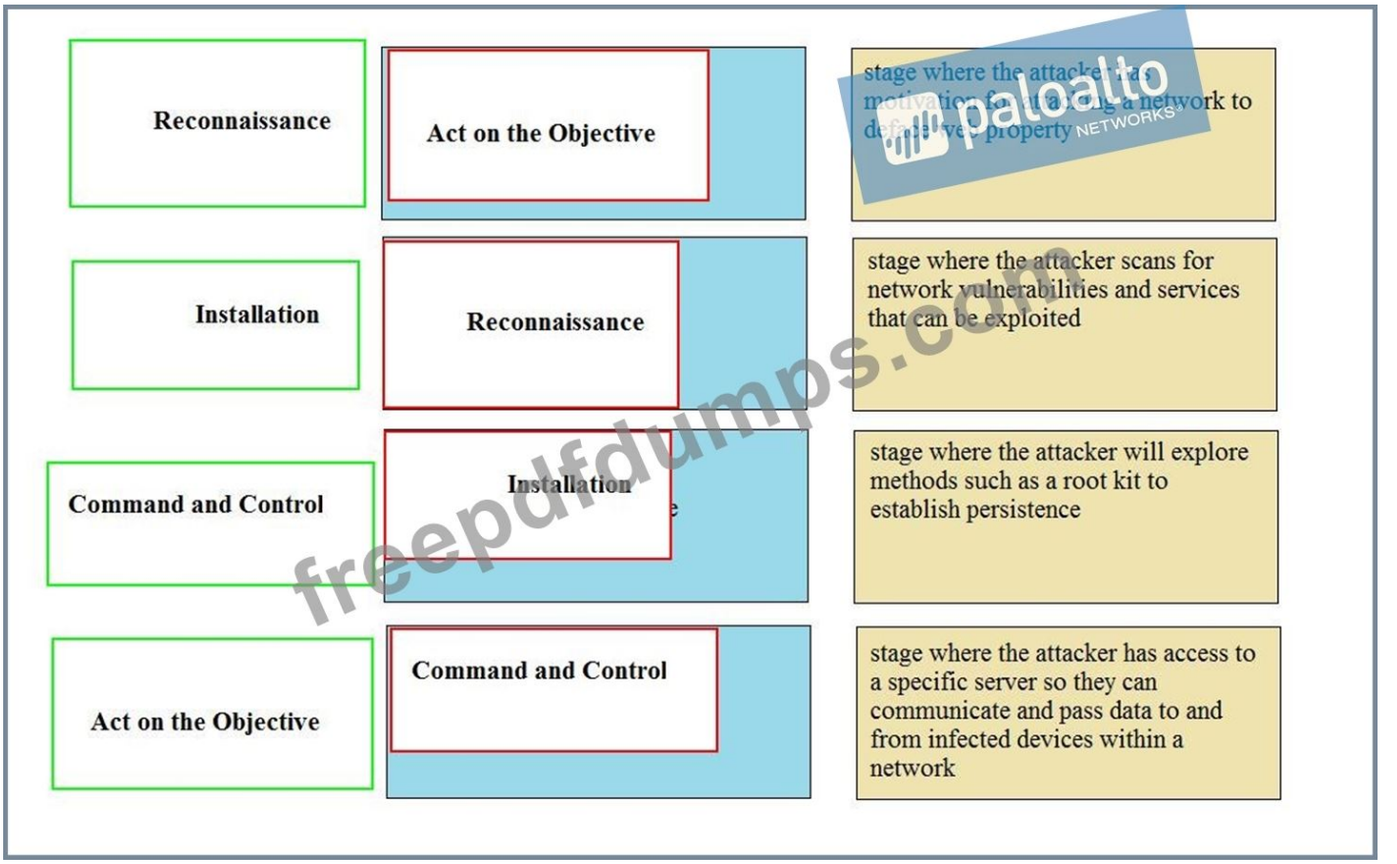
Answer: C (LEAVE A REPLY)

NEW QUESTION: 54

Match the Cyber-Attack Lifecycle stage to its correct description.



Answer:



NEW QUESTION: 55

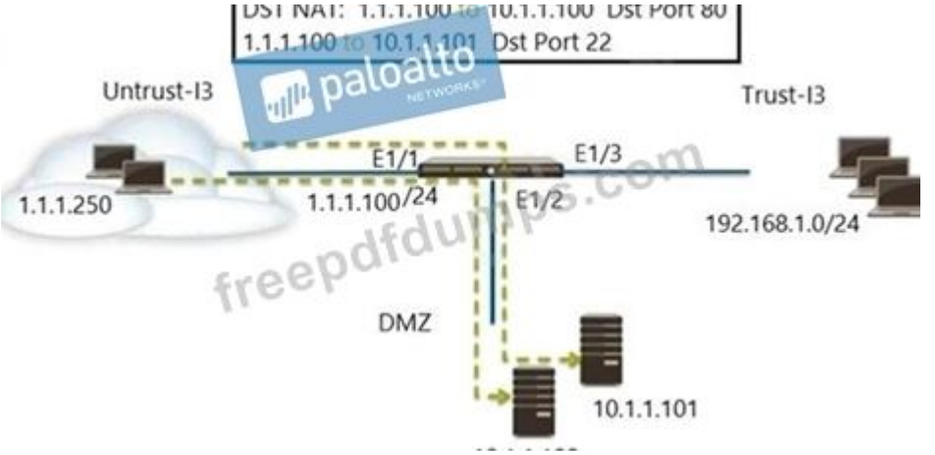
A network administrator created an intrazone Security policy rule on the firewall. The source zones were set to IT. Finance, and HR.
Which two types of traffic will the rule apply to? (Choose two)
A. traffic within zone HR
B. traffic within zone IT
C. traffic between zone Finance and zone HR
D. traffic between zone IT and zone Finance
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 56
To use Active Directory to authenticate administrators, which server profile is required in the authentication profile?
A. TACACS+
B. LDAP
C. domain controller
D. RADIUS
Answer: (SHOW ANSWER)

NEW QUESTION: 57
Which rule type is appropriate for matching traffic occurring within a specified zone?
A. Universal
B. Shadowed
C. Intrazone
D. Interzone
Answer: (SHOW ANSWER)

NEW QUESTION: 58
Your company occupies one floor in a single building you have two active directory domain controllers on a single networks the firewall s management plane is only slightly utilized.
Which user-ID agent sufficient in your network?
A. PAN-OS integrated agent deployed on the firewall
B. Windows-based agent deployed on the internal network a domain member
C. Citrix terminal server agent deployed on the network
D. Windows-based agent deployed on each domain controller
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/map-ip-addresses-to-users/configureuser-mapping-using-the-windows-user-id- agent/configure-the-windows-based-user-id- agent-for-usermapping.html

NEW QUESTION: 59
Refer to the exhibit. An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and Host B (10.1.1.101) receives SSH traffic.



Which two Security policy rules will accomplish this configuration? (Choose two.)
A. Untrust (Any)to DMZ (10.1.1.100. 10.1.1.101), ssh, web-browsing-Allow
B. Untrust (Any) to DMZ (1.1.1.100), web-browsing - Allow
C. Untrust (Any) to Untrust (10.1.1.1), web-browsing -Allow
D. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow
E. Untrust (Any) to DMZ (1.1.1.100), ssh - Allow
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 60
An administrator is troubleshooting an issue with traffic that matches the intrazone-default rule, which is set to default configuration.
What should the administrator do?
A. review the System Log
B. refresh the Traffic Log
C. change the logging action on the rule
D. tune your Traffic Log filter to include the dates
Answer: (SHOW ANSWER)

NEW QUESTION: 61
Which license must an Administrator acquire prior to downloading Antivirus Updates for use with the firewall?
A. Threat Environment License
B. Threat Protection License
C. Threat Implementation License
D. Threat Prevention License
Answer: (SHOW ANSWER)

NEW QUESTION: 62

Based on the screenshot what is the purpose of the included groups?

			Source			Destination				
	Name	Type	Zone	Address	User	Zone	Address	Application	Service	Action
1	allow-it	universal	inside	any	it	dmz	any	it-tools	application-default	Allow

A. They are only groups visible based on the firewall's credentials.

B. They are used to map usernames to group names.

C. They contain only the users you allow to manage the firewall.

D. They are groups that are imported from RADIUS authentication servers.

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Reference:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groups.html

NEW QUESTION: 63

The PowerBall Lottery has reached an unusually high value this week. Your company has decided to raise morale by allowing employees to access the PowerBall Lottery website (www.powerball.com) for just this week. However, the company does not want employees to access any other websites also listed in the URL filtering "gambling" category.

Which method allows the employees to access the PowerBall Lottery website but without unblocking access to the "gambling" URL category?

A. Add just the URL www.powerball.com to a Security policy allow rule.

B. Create a custom URL category, add *.powerball.com to it and allow it in the Security Profile.

C. Manually remove powerball.com from the gambling URL category.

D. Add *.powerball.com to the URL Filtering allow list.

Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 64

Which service protects cloud-based applications such as Dropbox and Salesforce by administering permissions and scanning files for sensitive information?

A. Aperture

B. GlobalProtect

C. Parisma SaaS
D. AutoFocus
Answer: (SHOW ANSWER)

NEW QUESTION: 65
Which three interface deployment methods can be used to block traffic flowing through the Palo Alto Networks firewall? (Choose three.)
A. Tap
B. Layer 3
C. Layer 2
D. Virtual Wire
E. HA
Answer: B,D,E (LEAVE A REPLY)

NEW QUESTION: 66
Which Palo Alto Networks firewall security platform provides network security for mobile endpoints by inspecting traffic deployed as internet gateways?
A. Aperture
B. AutoFocus
C. Panorama
D. GlobalProtect
Answer: (SHOW ANSWER)

NEW QUESTION: 67
Which firewall feature do you need to configure to query Palo Alto Networks service updates over a data-plane interface instead of the management interface?
A. Dynamic updates
B. SNMP setup
C. Service route
D. Data redistribution
Answer: C (LEAVE A REPLY)

NEW QUESTION: 68
Four configuration choices are listed, and each could be used to block access to a specific URL. If you configured each choices to block the sameURL then which choice would be the last to block access to the URL?
A. Custom URL category in Security Policy rule.
B. EDL in URL Filtering Profile.
C. Custom URL category in URL Filtering Profile.
D. PAN-DB URL category in URL Filtering Profile.
Answer: (SHOW ANSWER)

NEW QUESTION: 69
To what must an interface be assigned before it can process traffic?
A. Security Protection
B. Security policy
C. Security profile
D. Security Zone
Answer: D (LEAVE A REPLY)

NEW QUESTION: 70
What is a function of application tags?
A. application prioritization
B. creation of new zones
C. IP address allocations in DHCP
D. automated referenced applications in a policy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 71
Which Palo Alto networks security operating platform service protects cloud-based application such as Dropbox and salesforce by monitoring permissions and shared and scanning files for Sensitive information?
A. GlobalProtect
B. AutoFocus
C. Prisma SaaS
D. Panorama
Answer: C (LEAVE A REPLY)

NEW QUESTION: 72
What are three characteristics of the Palo Alto Networks DNS Security service? (Choose three.)
A. It requires an active subscription to a third-party DNS Security service.
B. It requires a valid Threat Prevention license.
C. It enables users to access real-time protections using advanced predictive analytics.
D. It uses techniques such as DGA.DNS tunneling detection and machine learning.
E. It requires a valid URL Filtering license.
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 73
Which action related to App-ID updates will enable a security administrator to view the existing security policy rule that matches new application signatures?
A. Review Policies
B. Review Apps

C. Pre-analyze
D. Review App Matches
Answer: A (LEAVE A REPLY)
References:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-new-app-ids-introduced- incontent-releases/review-new-app-id-impact-on- existing-policy-rules

NEW QUESTION: 74
Which two components are utilized within the Single-Pass Parallel Processing architecture on a Palo Alto Networks Firewall? (Choose two.)
A. User-ID
B. App-ID
C. Layer-ID
D. QoS-ID
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 75
Which statement is true regarding a Best Practice Assessment?
A. The assessment, guided by an experienced sales engineer, helps determine the areas of greatest risk where you should focus prevention activities
B. The BPA tool can be run only on firewalls
C. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture
D. It provides a percentage of adoption for each assessment data
Answer: A (LEAVE A REPLY)

NEW QUESTION: 76
Which URL Filtering profile action would you set to allow users the option to access a site only if they provide a URL admin password?
A. override
B. authorization
C. authentication
D. continue
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-filteringprofile-actions.html

NEW QUESTION: 77
Which built-in IP address EDL would be useful for preventing traffic from IP addresses that are verified as unsafe based on WildFire analysis Unit 42 research and data gathered from telemetry?
A. Palo Alto Networks C&C IP Addresses
B. Palo Alto Networks Bulletproof IP Addresses
C. Palo Alto Networks High-Risk IP Addresses
D. Palo Alto Networks Known Malicious IP Addresses
Answer: D (LEAVE A REPLY)
Palo Alto Networks Known Malicious IP Addresses
-Contains IP addresses that are verified malicious based on WildFire analysis, Unit 42 research, and data gathered from telemetry (Share Threat Intelligence with Palo Alto Networks). Attackers use these IP addresses almost exclusively to distribute malware, initiate command-and-control activity, and launch attacks.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/built-in-edls

NEW QUESTION: 78
Which administrator type provides more granular options to determine what the administrator can view and modify when creating an administrator account?
A. Dynamic
B. Root
C. Superuser
D. Role-based
Answer: (SHOW ANSWER)

NEW QUESTION: 79
Which security policy rule would be needed to match traffic that passes between the Outside zone and Inside zone, but does not match traffic that passes within the zones?
A. universal
B. intrazone
C. global
D. interzone
Answer: D (LEAVE A REPLY)

NEW QUESTION: 80
Which two Palo Alto Networks security management tools provide a consolidated creation of policies, centralized management and centralized threat intelligence. (Choose two.)
A. Panorama
B. GlobalProtect
C. AutoFocus
D. Aperture
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 81
An administrator would like to create a URL Filtering log entry when users browse to any gambling website. What combination of Security policy and Security profile actions is correct?
A. Security policy = allow. Gambling category in URL profile = allow
B. Security policy = allow, Gambling category in URL profile = alert
C. Security policy = deny. Gambling category in URL profile = block
D. Security policy = drop, Gambling category in URL profile = allow
Answer: (SHOW ANSWER)

NEW QUESTION: 82
Which type of security policy rule will match traffic that flows between the Outside zone and inside zone, but would not match traffic that flows within the zones?
A. global

B. intrazone
C. interzone
D. universal
Answer: C (LEAVE A REPLY)
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content-updates/dynamic- contentupdates.html#:~:text=WildFire%20signature%20updates%20are%20made,within%20a%20minute%20of %
20availability

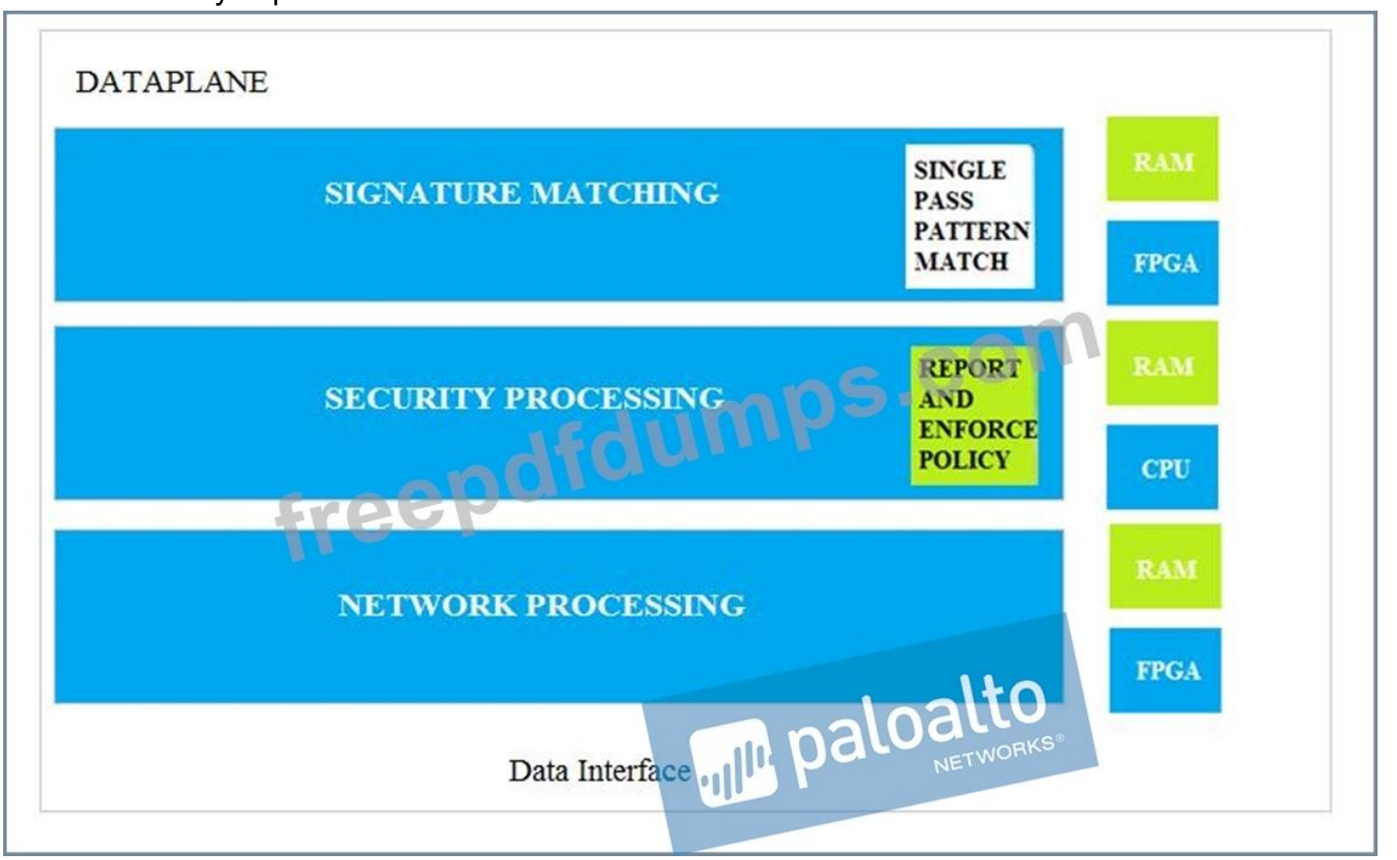
NEW QUESTION: 83
An administrator would like to use App-ID's deny action for an application and would like that action updated with dynamic updates as new content becomes available.
Which security policy action causes this?
A. Reset server
B. Reset both
C. Deny
D. Drop
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage-configuration backups/revert-firewall-configuration- changes.html

NEW QUESTION: 84
Given the detailed log information above, what was the result of the firewall traffic inspection?

A. It was blocked by the Vulnerability Protection profile action.
B. It was blocked by the Anti-Spyware Profile action.
C. It was blocked by the Security policy action.

D. It was blocked by the Anti-Virus Security profile action.
Answer: (SHOW ANSWER)

NEW QUESTION: 85
Which data-plane processor layer of the graphic shown provides uniform matching for spyware and vulnerability exploits on a Palo Alto Networks Firewall?



A. Signature Matching
B. Network Processing
C. Security Matching
D. Security Processing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 86
Which plane on a Palo alto networks firewall provides configuration logging and reporting functions on a separate processor?
A. network processing
B. management
C. security processing
D. data
Answer: B (LEAVE A REPLY)

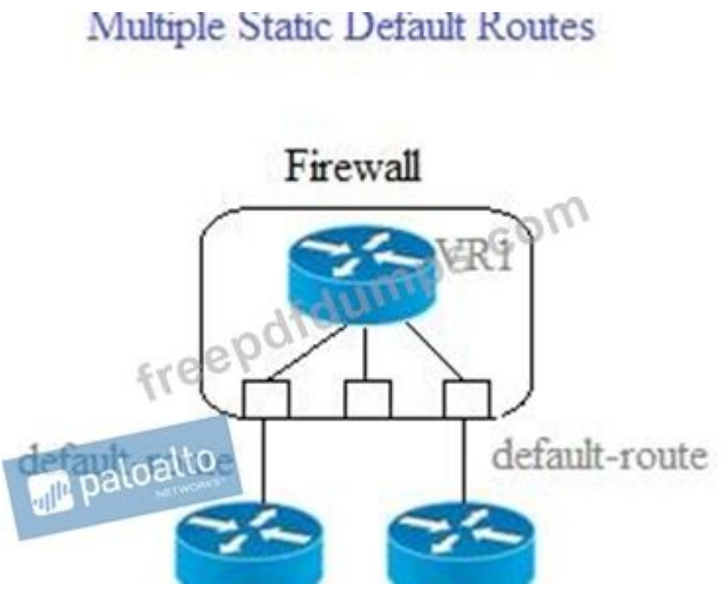
NEW QUESTION: 87
What must be configured before setting up Credential Phishing Prevention?

A. Anti Phishing Block Page
B. Threat Prevention
C. Anti Phishing profiles
D. User-ID
Answer: A (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing/set-up-credential-phishing-prevention

NEW QUESTION: 88
You need to allow users to access the office-suite application of their choice. How should you configure the firewall to allow access to any office-suite application?
A. Create an Application Filter and name it Office Programs, then filter it on the office programs subcategory.
B. Create an Application Group and add business-systems to it.
C. Create an Application Filter and name it Office Programs then filter on the business-systems category.
D. Create an Application Group and add Office 365, Evernote Google Docs and Libre Office
Answer: (SHOW ANSWER)

NEW QUESTION: 89
A network has 10 domain controllers, multiple WAN links, and a network infrastructure with bandwidth needed to support mission-critical applications. Given the scenario, which type of User-ID agent is considered a best practice by Palo Alto Networks?
A. Citrix terminal server with adequate data-plane resources
B. Captive Portal
C. Windows-based agent on a domain controller
D. PAN-OS integrated agent
Answer: C (LEAVE A REPLY)

NEW QUESTION: 90
Given the scenario, which two statements are correct regarding multiple static default routes? (Choose two.)



A. Path monitoring does not determine if route is useable
B. Route with highest metric is actively used
C. Path monitoring determines if route is useable
D. Route with lowest metric is actively used
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 91
Which interface does not require a MAC or IP address?
A. Layer3
B. Virtual Wire
C. Loopback
D. Layer2
Answer: B (LEAVE A REPLY)

NEW QUESTION: 92
An administrator is implementing an exception to an external dynamic list by adding an entry to the list manually. The administrator wants to save the changes, but the OK button is grayed out. What are two possible reasons the OK button is grayed out? (Choose two.)
A. The entry contains wildcards.
B. The entry is duplicated.

C. The entry doesn't match a list entry.
D. The entry matches a list entry.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 93
Users from the internal zone need to be allowed to Telnet into a server in the DMZ zone.
Complete the security policy to ensure only Telnet is allowed.
Security Policy: Source Zone: Internal to DMZ Zone _____services "Application defaults", and action = Allow
A. Destination IP: 192.168.1.123/24
B. Log Forwarding
C. USER-ID = 'Allow users in Trusted'
D. Application = 'Telnet'
Answer: D (LEAVE A REPLY)

NEW QUESTION: 94
Which action results in the firewall blocking network traffic without notifying the sender?
A. Drop
B. Deny
C. No notification
D. Reset Client
Answer: A (LEAVE A REPLY)

NEW QUESTION: 95
An administrator wants to prevent users from submitting corporate credentials in a phishing attack.
Which Security profile should be applied?
A. vulnerability protection
B. anti-spyware
C. antivirus
D. URL filtering
Answer: B (LEAVE A REPLY)

NEW QUESTION: 96
Which link in the web interface enables a security administrator to view the security policy rules that match new application signatures?
A. Review Policies
B. Review Apps
C. Review App Matches
D. Pre-analyze
Answer: A (LEAVE A REPLY)

NEW QUESTION: 97
During the packet flow process, which two processes are performed in application identification? (Choose two.)
A. pattern based application identification
B. session application identified
C. application override policy match
D. application changed from content inspection
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 98
Which statement is true regarding NAT rules?
A. Static NAT rules have precedence over other forms of NAT.
B. Translation of the IP address and port occurs before security processing.
C. Firewall supports NAT on Layer 3 interfaces only.
D. NAT rules are processed in order from top to bottom.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 99
When creating a Panorama administrator type of Device Group and Template Admin, which two things must you create first? (Choose two.)
A. admin rote
B. access domain
C. server profile
D. password profile
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 100
Which five Zero Trust concepts does a Palo Alto Networks firewall apply to achieve an integrated approach to prevent threats? (Choose five.)
A. Anti-spyware
B. Antivirus
C. User identification
D. Vulnerability protection
E. Application identification
F. Filtration protection
Answer: A,B,C,D,E (LEAVE A REPLY)

NEW QUESTION: 101
What do you configure if you want to set up a group of objects based on their ports alone?
A. Application groups

B. Custom objects
C. Service groups
D. Address groups
Answer: C (LEAVE A REPLY)

NEW QUESTION: 102
An administrator configured a Security policy rule where the matching condition includes a single application and the action is set to deny. What deny action will the firewall perform?
A. Discard the session's packets and send a TCP reset packet to let the client know the session has been terminated
B. Perform the default deny action as defined in the App-ID database for the application
C. Drop the traffic silently
D. Send a TCP reset packet to the client- and server-side devices
Answer: A (LEAVE A REPLY)

NEW QUESTION: 103
An administrator has an IP address range in the external dynamic list and wants to create an exception for one specific IP address in this address range.
Which steps should the administrator take?
A. Add the address range to the Manual Exceptions list and exclude the IP address by selecting the entry.
B. Select the address range in the List Entries list. A column will open with the IP addresses. Select the entry to exclude.
C. Add the specific IP address from the address range to the Manual Exceptions list by using regular expressions to define the entry.
D. Add each IP address in the range as a list entry and then exclude the IP address by adding it to the Manual Exceptions list.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 104
What does an application filter help you to do?
A. It dynamically shapes defined application traffic based on active sessions and bandwidth usage.
B. It dynamically filters applications based on critical, high, medium, low. or informational severity.
C. It dynamically provides application statistics based on network, threat, and blocked activity,
D. It dynamically groups applications based on application attributes such as category and subcategory.
Answer: (SHOW ANSWER)

NEW QUESTION: 105
When creating a custom URL category object, which is a valid type?

A. domain match
B. category match
C. host names
D. wildcard
Answer: B (LEAVE A REPLY)

NEW QUESTION: 106
Your company requires positive username attribution of every IP address used by wireless devices to support a new compliance requirement. You must collect IP -to-user mappings as soon as possible with minimal downtime and minimal configuration changes to the wireless devices themselves. The wireless devices are from various manufactures.
Given the scenario, choose the option for sending IP-to-user mappings to the NGFW.
A. RADIUS
B. syslog
C. XFF headers
D. UID redistribution
Answer: (SHOW ANSWER)

NEW QUESTION: 107
Access to which feature requires the PAN-OS Filtering license?
A. Custom URL categories
B. DNS Security
C. PAN-DB database
D. URL external dynamic lists
Answer: (SHOW ANSWER)

NEW QUESTION: 108
Which Security profile must be added to Security policies to enable DNS Signatures to be checked?
A. Anti-Spyware
B. Antivirus
C. URL Filtering

D. Vulnerability Protection
Answer: (SHOW ANSWER)

NEW QUESTION: 109
Access to which feature requires PAN-OS Filtering licens?
A. Custom URL categories
B. DNS Security
C. URL external dynamic lists
D. PAN-DB database
Answer: D (LEAVE A REPLY)

NEW QUESTION: 110
Which license is required to use the Palo Alto Networks built-in IP address EDLs?
A. DNS Security
B. Threat Prevention
C. WildFire
D. SD-Wan
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/use-an-external-dynamic-list-in- policy/builtin-edls.html#:~:text=With%20an%

NEW QUESTION: 111
What do dynamic user groups you to do?
A. create a QoS policy that provides auto-remediation for anomalous user behavior and malicious activity
B. create a policy that provides auto-sizing for anomalous user behavior and malicious activity
C. create a policy that provides auto-remediation for anomalous user behavior and malicious activity
D. create a dynamic list of firewall administrators
Answer: C (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups#:~:text=Dynamic%20user%20groups%20help%20you,activity%20while%20maintaining%20user%20visibility.

NEW QUESTION: 112
The Palo Alto Networks NGFW was configured with a single virtual router named VR-1 What changes are required on VR-1 to route traffic between two interfaces on the NGFW?
A. Add zones attached to interfaces to the virtual router
B. Add a static routes to route between the two interfaces

C. Add interfaces to the virtual router
D. Enable the redistribution profile to redistribute connected routes
Answer: (SHOW ANSWER)

NEW QUESTION: 113
Which two statements are true for the DNS security service introduced in PAN-OS version 10.0?
A. IT eliminates the need for dynamic DNS updates.
B. It removes the 100K limit for DNS entries for the downloaded DNS updates.
C. It functions like PAN-DB and requires activation through the app portal.
D. IT is automatically enabled and configured.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 114
A company moved its old port-based firewall to a new Palo Alto Networks NGFW 60 days ago. Which utility should the company use to identify out-of-date or unused rules on the firewall?
A. Rule Usage Filter > No App Specified
B. Rule Usage Filter > Unused Apps
C. Rule Usage Filter >Hit Count > Unused in 30 days
D. Rule Usage Filter > Hit Count > Unused in 90 days
Answer: D (LEAVE A REPLY)

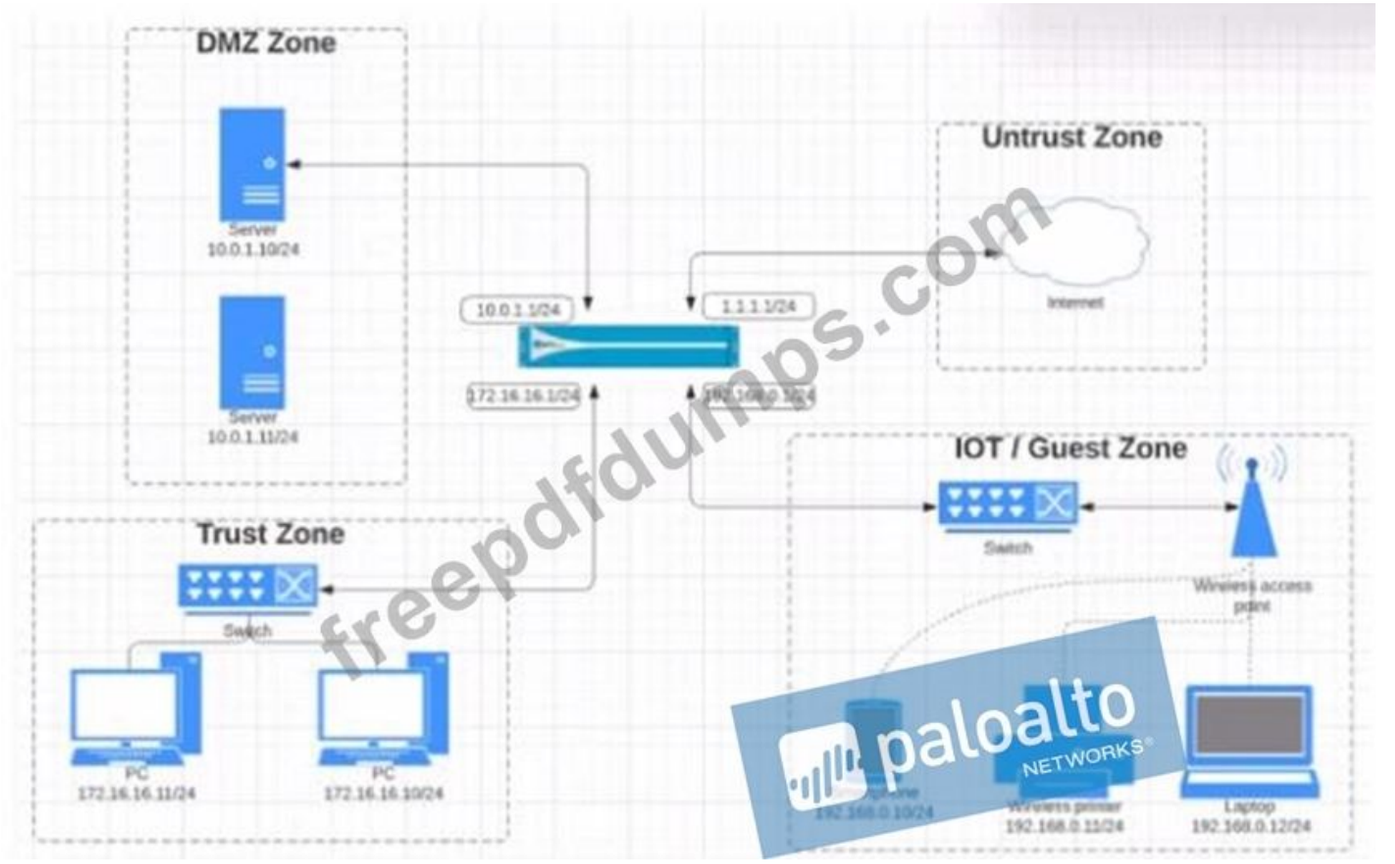
NEW QUESTION: 115
Which interface type is part of a Layer 3 zone with a Palo Alto Networks firewall?
A. Aggregate
B. Aggregation
C. Management
D. High Availability
Answer: A (LEAVE A REPLY)

NEW QUESTION: 116
Which object would an administrator create to enable access to all applications in the office-programs subcategory?
A. HIP profile
B. Application filter
C. Application group
D. URL category
Answer: (SHOW ANSWER)

NEW QUESTION: 117
Which administrative management services can be configured to access a management interface?

A. HTTP, CLI, SNMP, HTTPS
B. HTTPS, SSH telnet SNMP
C. SSH: telnet HTTP, HTTPS
D. HTTPS, HTTP. CLI, API
Answer: D (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/management-interfaces You can use the following user interfaces to manage the Palo Alto Networks firewall:
Use the Web Interface to perform configuration and monitoring tasks with relative ease. This graphical interface allows you to access the firewall using HTTPS (recommended) or HTTP and it is the best way to perform administrative tasks.
Use the Command Line Interface (CLI) to perform a series of tasks by entering commands in rapid succession over SSH (recommended), Telnet, or the console port. The CLI is a no-frills interface that supports two command modes, operational and configure, each with a distinct hierarchy of commands and statements. When you become familiar with the nesting structure and syntax of the commands, the CLI provides quick response times and administrative efficiency.
Use the XML API to streamline your operations and integrate with existing, internally developed applications and repositories. The XML API is a web service implemented using HTTP/HTTPS requests and responses.
Use Panorama to perform web-based management, reporting, and log collection for multiple firewalls. The Panorama web interface resembles the firewall web interface but with additional functions for centralized management.

NEW QUESTION: 118
View the diagram. What is the most restrictive, yet fully functional rule, to allow general Internet and SSH traffic into both the DMZ and Untrust/Internet zones from each of the lOT/Guest and Trust Zones?



A.

B.

C.

D.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 119

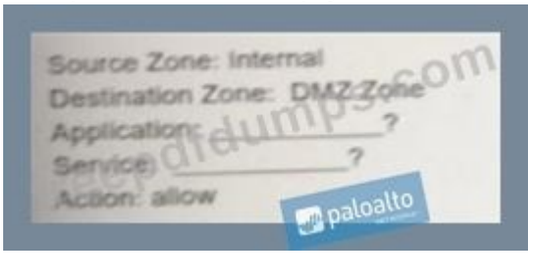
Which two rule types allow the administrator to modify the destination zone? (Choose two)

A. interzone

B. universal
C. intrazone
D. shadowed
Answer: (SHOW ANSWER)

NEW QUESTION: 120
Which path is used to save and load a configuration with a Palo Alto Networks firewall?
A. Device>Setup>Management
B. Device>Setup>Services
C. Device>Setup>Operations
D. Device>Setup>Interfaces
Answer: C (LEAVE A REPLY)

NEW QUESTION: 121
All users from the internal zone must be allowed only Telnet access to a server in the DMZ zone.
Complete the two empty fields in the Security Policy rules that permits only this type of access.



Choose two.
A. Application = "any"
B. Application = "Telnet"
C. Service = "any"
D. Service - "application-default"
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 122
In the example security policy shown, which two websites fcked? (Choose two.)

	Name	Tags	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Block-Sites	outbound	Inside	Any	Outside	Any	Any	any	Social-networking	Deny	None

A. YouTube
B. Amazon
C. Facebook
D. LinkedIn
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 123
The NetSec Manager asked to create a new firewall Local Administrator profile with customized privileges named NewAdmin. This new administrator has to authenticate without inserting any username or password to access the WebUI.
What steps should the administrator follow to create the New_Admin Administrator profile?
A. 1. Select the "Use only client certificate authentication" check box.
2. Set Role to Role Based.
3. Issue to the Client a Certificate with Common Name = NewAdmin
B. 1. Set the Authentication profile to Local.
2. Select the "Use only client certificate authentication" check box.
3. Set Role to Role Based.
C. 1. Select the "Use only client certificate authentication" check box.
2. Set Role to Dynamic.
3. Issue to the Client a Certificate with Common Name = New Admin
D. 1. Select the "Use only client certificate authentication" check box.
2. Set Role to Dynamic.
3. Issue to the Client a Certificate with Certificate Name = NewAdmin
Answer: D (LEAVE A REPLY)

NEW QUESTION: 124
If using group mapping with Active Directory Universal Groups, what must you do when configuring the User-ID?
A. Create an LDAP Server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSL
B. Configure a frequency schedule to clear group mapping cache
C. Configure a Primary Employee ID number for user-based Security policies
D. Create a RADIUS Server profile to connect to the domain controllers using LDAPS on port 636 or 389
Answer: (SHOW ANSWER)

If you have Universal Groups, create an LDAP server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSL, then create another LDAP server profile to connect to the root domain controllers on port 389. This helps ensure that users and group information is available for all domains and subdomains.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groups

NEW QUESTION: 125
Which type of administrative role must you assign to a firewall administrator account, if the account must include a custom set of firewall permissions?
A. Dynamic
B. Multi-Factor Authentication
C. SAML
D. Role-based
Answer: D (LEAVE A REPLY)

NEW QUESTION: 126
What can be achieved by selecting a policy target prior to pushing policy rules from Panorama?
A. Doing so limits the templates that receive the policy rules
B. You specify the location as pre can - or post-rules to push policy rules
C. You can specify the firewalls m a device group to which to push policy rules
D. Doing so provides audit information prior to making changes for selected policy rules
Answer: C (LEAVE A REPLY)

NEW QUESTION: 127
Based on the security policy rules shown, ssh will be allowed on which port?

			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

A. 22
B. 80
C. 23
D. 53
Answer: (SHOW ANSWER)

NEW QUESTION: 128

Which protocol used to map username to user groups when user-ID is configured?
A. RADIUS
B. SAML
C. TACACS+
D. LDAP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 129
What is the purpose of the automated commit recovery feature?
A. It causes HA synchronization to occur automatically between the HA peers after a push from Panorama.
B. It generates a config log after the Panorama configuration successfully reverts to the last running configuration.
C. It reverts the firewall configuration if the firewall recognizes a loss of connectivity to Panorama after the change.
D. It reverts the Panorama configuration.
Answer: (SHOW ANSWER)